1 (10%) Eve installed some soywars software on 100 LIGD Bash doves and has designed this software to autoload in a Windows systers from these drives along with como nude photos. She then painted the logo of a well- known adult magazine on each one and randomly scattered these flash drives in the parking lots of several of the big defense companies in her town What type of malware attack is this and what vunerability in she trying to exploit to these companies?

Ans1. The scenario described in the question is an example of a "baiting" attack, which is a social engineering technique used to trick people into opening malware-infected files or devices.

In this case, Eve is using flash drives with enticing content (nude photos) and a recognizable logo to lure unsuspecting employees of big defense companies to insert them into their computers. Once the flash drive is inserted, the malware will automatically load onto the Windows system, infecting it with the soywars software.

The vulnerability that Eve is trying to exploit is the human factor - employees who are curious or tempted by the content on the flash drive may not be aware of the risks of inserting an unknown device into their computer. By doing so, they may inadvertently compromise their organization's security by introducing malware that can steal sensitive information or give attackers unauthorized access to their systems.

2. (25%) Assuming an attacker has compromised a number of broadband

ecnected comput o use as zombie systems for a distributed denial of

service (DDOS) attack if the ISP provides a maximum uplink data rate of

7.5 Mips in in cable service, what is the maximum number of 256-byte

ICMP echo request (ping) packets a single zombie computer can send per

second? How many such zombie systems would the attacker need to

food a target server connected in

(a)A Fast Ethernet

(b) A Gigabit Ethernet

Ans2. To calculate the maximum number of 256-byte ICMP echo request (ping) packets a single zombie computer can send per second, we need to first calculate the maximum data rate in bits per second for the 7.5 Mbps uplink data rate provided by the ISP.

Maximum data rate = 7.5 Mbps = 7,500,000 bits per second

To calculate the maximum number of packets that can be sent per second, we need to consider the overhead of the packet headers. An ICMP echo request packet has a 20-byte IP header and an 8-byte ICMP header in addition to the 256-byte payload. So, the total size of each packet is 284 bytes.

Maximum packets per second = (maximum data rate in bits per second) / (packet size in bits)

= (7,500,000 bps) / (284 bytes \* 8 bits/byte)

= 3,308 packets per second

So, a single zombie computer can send up to 3,308 256-byte ICMP echo request packets per second.

Now, let's calculate the number of zombie systems the attacker would need to flood a target server connected in (a) a Fast Ethernet and (b) a Gigabit Ethernet.

(a) Fast Ethernet has a maximum data rate of 100 Mbps, which is 100,000,000 bits per second.

Number of zombie systems needed = (maximum data rate of target server in bits per second) / (maximum data rate of a single zombie system in bits per second)

= (100,000,000 bps) / (3,308 bps)

= 30,244 zombie systems (rounded up)

So, the attacker would need approximately 30,244 zombie systems to flood a target server connected in Fast Ethernet.

(b) Gigabit Ethernet has a maximum data rate of 1 Gbps, which is 1,000,000,000 bits per second.

Number of zombie systems needed = (maximum data rate of target server in bits per second) / (maximum data rate of a single zombie system in bits per second)

= (1,000,000,000 bps) / (3,308 bps)

= 302,440 zombie systems (rounded up)

So, the attacker would need approximately 302,440 zombie systems to flood a target server connected in Gigabit Ethernet.

3. (25%) A password system uses exact 8-character of alphanumane. To be

a secure password system, any password cannot contain the following

keywords

(a) All numbers. Le, must contain at least one letter in the password

(b) User's name.

What is the probability of an adversary guessing John Hank's password

correctly?

Ans3. Assuming that the password system requires exactly 8 characters that must be alphanumeric and cannot contain all numbers or the user's name, we can calculate the probability of an adversary guessing John Hank's password correctly as follows:

(a) All numbers

There are 10 possible digits (0-9) that can be used in the password, and each position can be filled with any of these digits. Therefore, there are 10^8 possible passwords consisting only of numbers.

However, since the password cannot contain all numbers, we need to subtract the number of passwords that consist only of numbers from the total number of possible passwords:

Number of passwords consisting only of numbers = 10^8 - 10 = 99,999,990

The probability of an adversary guessing John Hank's password correctly if he uses a password consisting only of numbers is 1 in 99,999,990.

(b) User's name

Assuming that John Hank's name consists of two words, we can calculate the total number of possible passwords that contain his name by considering all possible positions and combinations of the letters in his name:

Number of possible passwords containing John Hank's name = (8 choose 2) \* 26^6 \* 2^2 = 26,702,754,304

where (8 choose 2) is the number of ways to choose 2 positions out of 8 for the letters in John and Hank, 26^6 is the number of possible combinations of 6 letters in the remaining positions (since the password must be alphanumeric), and 2^2 is the number of ways to arrange the two words in the password.

The probability of an adversary guessing John Hank's password correctly if he uses a password containing his name is 1 in 26,702,754,304.

Therefore, the probability of an adversary guessing John Hank's password correctly if he follows the password system's requirements and does not use a password consisting only of numbers or his name is the combined probability of (a) and (b), which is:

Probability = 1 / (99,999,990 \* 26,702,754,304) = 3.745 x 10^-19

So the probability of an adversary guessing John Hank's password correctly is extremely low (less than 1 in a billion billion).

4. (20%) Consider user accounts on a computer system with a Web server configured to provide user Web areas. In general, this usos a standard directory name, such as "public\_html" in a user's home directory. However, access control needs to be properly set to allow users (with or without user accounts on the system) to browse the webpages. Assuming there are one main page (index.html), two pictures files (a.jpg and b.jpg) stored in an sub-directory (Image) and one pdf file (cpat) stored in an sub- directory (Doc), all under the public\_html.

(a)Specify the access matrix for each directory (excluding the user's home directory) and tiles that allows everyone to view the webpage

(b)Draw a directed graph that represented to the access matrix

Ans 4. (a) Access matrix for each directory:

public\_html: owner(rwx), group(r-x), others(r-x)

public\_html/Image: owner(rwx), group(r-x), others(r-x)

public\_html/Image/a.jpg: owner(rwx), group(r-x), others(r-x)

public\_html/Image/b.jpg: owner(rwx), group(r-x), others(r-x)

public\_html/Doc: owner(rwx), group(r-x), others(r-x)

public\_html/Doc/cpat: owner(rwx), group(r-x), others(r-x)

To allow everyone to view the webpage, the permissions for the directories and files can be set as follows:

public\_html: owner(rwx), group(r-x), others(r-x)

public\_html/Image: owner(rwx), group(r-x), others(r-x)

public\_html/Image/a.jpg: owner(rwx), group(r-x), others(r--), read permission added for others

public\_html/Image/b.jpg: owner(rwx), group(r-x), others(r--), read permission added for others

public\_html/Doc: owner(rwx), group(r-x), others(r-x)

public\_html/Doc/cpat: owner(rwx), group(r-x), others(r--), read permission added for others

(b) Directed graph representation of access matrix:

public\_html -> Image -> a.jpg

| -> b.jpg

|-> Doc -> cpat

Q5.

Ans 5. a.

Rule A: Permits incoming HTTP traffic from external to internal network.

Rule B: Permits outgoing HTTP traffic from internal to external network.

Rule C: Permits outgoing HTTP traffic from internal to external network.

Rule D: Permits incoming HTTP traffic from external to internal network.

Rule E: Denies any traffic.

b.

Packet 1: Denied by Rule E, since it is trying to establish a connection with no specific source or destination address.

Packet 2: Permitted by Rule B, since it is an outgoing HTTP traffic from an internal host to an external host on port 80.

Packet 3: Permitted by Rule C, since it is an outgoing HTTP traffic from an internal host to an external host on port 80.

Packet 4: Permitted by Rule D, since it is an incoming HTTP traffic from an external host to an internal host on port greater than 1023.

c.

The attack will not succeed because it is trying to establish a connection to the web proxy server on port 8080, while the access rule set is only allowing inbound and outbound HTTP traffic on port 80. Therefore, Packet 5 will be denied by default, and no further packets will be allowed to establish a connection on port 8080.